

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Three Samsung Cellular Phones, currently in the
possession of the U.S. Probation Office in Seattle,
Washington, as further described in Attachment A

Case No. MJ18-117

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
Three Samsung Cellular Phones, as further described in Attachment A

located in the Western District of Washington, there is now concealed (identify the person or describe the property to be seized):
See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC 2252	Possession, Distribution, Receipt of Child Pornography
18 USC 2422	Attempted Enticement of a Minor

The application is based on these facts:
See Affidavit of SA Gabriel Stajduhar, attached hereto and incorporated by reference.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Gabriel Stajduhar, Special Agent, HSI
Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: 3/16/18


Judge's signature

City and state: Seattle, Washington

Brian A. Tsuchida, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
)
COUNTY OF KING) ss

I, Gabriel Stajduhar, being duly sworn on oath, depose and state:

INTRODUCTION AND AGENT BACKGROUND

1. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). I have been so employed since 2006. I am currently assigned to the Tacoma, Washington Office of the Special Agent in Charge (SAC) in Seattle, Washington. Homeland Security Investigations (HSI) is responsible for enforcing customs and immigration laws and federal criminal statutes of the United States. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including the production, distribution, receipt, and possession of child pornography and material involving the sexual exploitation of minors in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I graduated from the Federal Law Enforcement Training Center (FLETC), ICE Special Agent Training Program, and I received further specialized training in investigating, child pornography and child exploitation crimes. I have also had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256(8)). I have participated in the execution dozens of previous search warrants that involved child exploitation and/or child pornography offenses. I have been a full time computer forensic agent for over three years. I attended and completed Homeland Security Investigation's six week computer and digital media forensics program. I also have attended advanced training on cellular/digital forensics. I have forensically extracted and examined over a hundred cellular phones. I also have completed well over a hundred forensic extractions of computer hard drives and other digital devices. Most of these investigations have been related to the possession and/or distribution of child pornography.

2. I am submitting this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following cellular phones: a Samsung SM-S120L (IMEI 359259076055077), a Samsung SM-S727VL (IMEI 354727083181461), and a Samsung Galaxy (missing identification sticker) (collectively the "SUBJECT PHONES"). The SUBJECT PHONES were found in the possession of PETER JAMES HUFFERD and they are currently located in the United States Probation Office in Seattle, Washington. These items are more fully described in Attachment A. I request authority to search the SUBJECT PHONES for the things specified in Attachment B to this Affidavit, for the reasons set forth below.

3. The warrant would authorize a search, seizure, and forensic examination of the Cellular Phones, for the purpose of identifying electronically stored data as particularly described in Attachment B, for evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) and 18 U.S.C. § 2422(b) (Attempted Enticement of a Minor).

4. The facts set forth in this Application for Search Warrant are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation (including the United States Probation Service (USPO)), my review of documents and records related to this investigation and a previous investigation of PETER JAMES HUFFERD, communications with others who have personal knowledge of the events and circumstances described herein, and my training and experience. Because this affidavit is offered for the limited purpose of establishing probable cause, I list only those facts that I believe are necessary to support such a finding. I do not purport to list every fact known to me or others as a result of this investigation.

//

//

STATEMENT OF PROBABLE CAUSE

A. Background of PETER JAMES HUFFERD

5. In February of 2008, the King County Sheriff's Office (KCSO) and the United States Veterans Affairs, Office of Inspector General (VA-OIG) initiated a child enticement investigation. I reviewed a Complaint filed in United States District Court as a result of this investigation. As part of this enticement investigation, according to the sworn complaint, a VA agent reviewed a Port Angeles police report from 2003. In this report, PETER JAMES HUFFERD admitted to officers that he had chatted with minor females using the name "LisaJones12345." In 2003, HUFFERD was convicted of three counts of Possession of Depictions of Minors Engaged in Sexually Explicit Conduct in Clallam County Superior Court and sentenced to 115 days in custody.

6. The 2008 enticement investigation began when a 12-year-old female's father complained that his daughter was having online sexual conversations with a person known as "Lisa Jones." According to the complaint, "Lisa Jones" attempted to get the minor female to converse with adult males and set up meetings. "Lisa Jones" convinced the minor female to cut herself and hide the cuts from her parents. "Lisa Jones" also wrote to the minor female about sexual acts.

7. Investigators traced the "Lisa Jones" online account to HUFFERD. In March 2008, HUFFERD was living in VA housing in Lakewood, Washington. That same month, investigators obtained a search warrant for HUFFERD's computer. During the subsequent search of HUFFERD's computer, investigators found over 300 images and 9 videos that child pornography¹, or depictions of minors engaged in sexually explicit conduct.

8. On July 23, 2008, HUFFERD was arrested based on the aforementioned complaint and charged in the Western District of Washington with Possession of Child Pornography. On February 18, 2009, HUFFERD pleaded guilty one count of Possession of Child Pornography in , in violation of Title 18, United States Code Sections

¹ For purposes of this Affidavit, I use the definition of child pornography found at 18 U.S.C. § 2256(8), which is, in summary, a visual depiction of sexually explicit conduct the production of which involves the use of a minor.

2252A(a)(5)(B) and 2252A(b)(2). In the Plea Agreement, HUFFERD admitted that he possessed more than 300 images and 9 videos of child pornography. On May 14, 2009, the Honorable Judge Ronald B. Leighton sentenced HUFFERD to 120 months' imprisonment and 20 years' supervised release.

B. Current Investigation

9. HUFFERD's term of supervised release commenced on April 7, 2017, in the Western District of Washington. According to the judgment in the 2008 case, HUFFERD was subject to several special conditions of supervised release, including, but not limited to:

- A) a requirement that HUFFERD submit his person, residence, and property to search by the probation office;
- B) a requirement that HUFFERD shall not possess any material that depicts sexually explicit conduct;
- C) a requirement that HUFFERD have not direct or indirect contact with children under the age of 18; and
- D) a requirement that the probation office monitor HUFFERD's computers and electronic media.

10. For the past several months, HUFFERD has been supervised by United States Probation Officer (USPO) Sarah Cavendish. HUFFERD has resided in a Seattle halfway house that provided housing for sex offenders. In November 2017, USPO Cavendish received information that HUFFERD was in possession of multiple cellular phones with pornography on them. HUFFERD was then ordered to take a polygraph which he passed in December of 2017.

11. In February 2018, USPO Cavendish received a report that HUFFERD was viewing pornography on a television. On March 9, 2018, HUFFERD's room at the Seattle halfway house was searched by the USPO. According to USPO Cavendish, HUFFERD admitted to having undisclosed cellular phones along with his previously approved cellular phones. HUFFERD admitted to USPO Cavendish that he had been

viewing pornography for the past two months on the undisclosed cellular phones. He admitted daily viewing of pornography. When asked if it was adult or child pornography, HUFFERD stated that he “thinks” all of the pornography viewed was of adults.

12. HUFFERD further admitted to communicating with minor females through the social media sites Tumblr and Instagram. When asked what type of communication he was having with the minors he responded “everything.” HUFFERD then made admissions that the conversations with the minor females were sexual in nature.

13. The USPO began a review of HUFFERD’s cellular phones. On one of the SUBJECT PHONES, another USPO officer showed pictures from a Tumblr social media account to USPO Cavendish; USPO Cavendish believed the pictures contained females who were approximately 13-14 years old. The probation review of the SUBJECT PHONES was stopped in favor of law enforcement review.

14. During the probation contact, HUFFERD also made statements that “I am fucked and going away for another 20 years.” HUFFERD was then arrested on violation of his probation. During his transport to the Tacoma Federal Courthouse, HUFFERD made additional statements that “it’s over” and “I am going away for a long time, but I did it to myself.”

15. In total, the USPO located four cellular phones. Once phone was a LG flip phone that was determined to be non-working. The LG flip phone is not included in this application for a search warrant. However, it does appear that one of three SUBJECT PHONES was the cellular phone that was monitored by the Probation Office. Although this phone could be searched without a warrant (as could all of the phones based on supervision conditions), I am including this phone in this application for completeness. Based on the totality of the circumstances, including HUFFERD’s evasive behavior I believe that there is probable cause to search the monitored for evidence related to the subject crimes (for example other contact with minor females or evidence related to that contact, e.g., travel arrangements, gift purchases).

//

TECHNICAL BACKGROUND .

16. Based on my training and experience, I have learned that the computer, including a cellular phone, has the ability to store images and videos in digital form. Based on my training and experience, collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by companies such as Google, Yahoo, Apple, and Dropbox, among others. The online services allow a user to set up an account with a remote computing service that provides email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer, including a cellular phone. And even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer/cellular phone in most cases.

17. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer (or cellular phone) used for these purposes. Storing this information can be intentional, i.e., by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" and history files of the browser application used. A forensic examiner often can recover evidence suggesting whether a computer contains wireless software, and when certain files under investigation were uploaded or downloaded. Such information is often maintained indefinitely until overwritten by other data.

18. Based on my training and experience, I have learned that producers of child pornography can produce image and video digital files from the average digital camera, cellular phone, or tablet. These files can then transferred from the mobile device to a

computer or other digital device, using the various methods described above. The digital files can then be stored, manipulated, transferred, or printed directly from a computer or other digital device, including a cellular phone. Digital files can also be edited in ways similar to those by which a photograph may be altered; they can be lightened, darkened, cropped, or otherwise manipulated. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the child pornographer in that this method of production is a difficult trail for law enforcement to follow.

19. As part of my training and experience, I have become familiar with the structure of the Internet, and I know that connections between computers on the Internet routinely cross state and international borders, even when the computers communicating with each other are in the same state. Individuals and entities use the Internet to gain access to a wide variety of information; to send information to, and receive information from, other individuals; to conduct commercial transactions; and to communicate via email.

20. Based on my training and experience, I know that cellular mobile phones (often referred to as "smart phones") have the capability to access the Internet and store information, such as images and videos. As a result, an individual using a smart phone can send, receive, and store files, including child pornography, without accessing a personal computer or laptop. An individual using a smart phone can also easily connect the device to a computer or other digital device, via a USB or similar cable, and transfer data files from one digital device to another.

21. As set forth herein and in Attachment B to this Affidavit, I seek permission to search for and seize evidence, fruits, and instrumentalities of the above-referenced crimes that might be found in the SUBJECT PHONES in whatever form they are found. It has been my experience that individuals involved in child pornography often prefer to store images of child pornography in electronic form. The ability to store images of child pornography in electronic form makes digital devices an ideal repository for child

pornography because the images can be easily sent or received over the Internet. As a result, one form in which these items may be found is as electronic evidence stored on a digital device.

22. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to individuals who have a sexualized interest in children and depictions of children:

a. They may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. They may collect sexually explicit or suggestive materials in a variety of media. Such individuals often times use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts. These individuals may keep records, to include names, contact information, and/or dates of these interactions, of the children they have attempted to seduce, arouse, or with whom they have engaged in the desired sexual acts.

c. They often maintain any “hard copies” of child pornographic material that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These individuals typically retain these “hard copies” of child pornographic material for many years, as they are highly valued.

d. Likewise, they often maintain their child pornography collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, often at the individual’s residence or some otherwise easily accessible location, to enable the owner to view the collection, which is valued highly.

They also may opt to store the contraband in cloud accounts. Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage can span multiple servers, and often locations, and the physical environment is typically owned and managed by a hosting company. Cloud storage allows the offender ready access to the material from any device that has an Internet connection, worldwide, while also attempting to obfuscate or limit the criminality of possession as the material is stored remotely and not on the offender's device.

e. They also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. They generally prefer not to be without their child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.

g. E-mail itself provides a convenient means by which individuals can access a collection of child pornography from any computer, at any location with Internet access. Such individuals therefore do not need to physically carry their collections with them but rather can access them electronically. Furthermore, these collections can be stored on email "cloud" servers, which allow users to store a large amount of material at no cost, without leaving any physical evidence on the users' computer(s).

23. In addition to offenders who collect and store child pornography, law enforcement has encountered offenders who obtain child pornography from the internet, view the contents and subsequently delete the contraband, often after engaging in self-gratification. In light of technological advancements, increasing Internet speeds and worldwide availability of child sexual exploitative material, this phenomenon offers the offender a sense of decreasing risk of being identified and/or apprehended with quantities

of contraband. This type of consumer is commonly referred to as a 'seek and delete' offender, knowing that the same or different contraband satisfying their interests remain easily discoverable and accessible online for future viewing and self-gratification. I know that, regardless of whether a person discards or collects child pornography he/she accesses for purposes of viewing and sexual gratification, evidence of such activity is likely to be found on computers and related digital devices used by the person. This evidence may include the files themselves, logs of account access events, contact lists of others engaged in trafficking of child pornography, backup files, and other electronic artifacts that may be forensically recoverable.

24. Given the above, including the criminal history of PETER JAMES HUFFERD, his prior contacts with minor females, his recent admissions about viewing pornography that he "thinks" is adult, and his admissions about recently contacting minor females and engaging in sexual discussions, and based on my knowledge, training and experience, along with my discussions with other law enforcement officers who investigate child exploitation crimes, I believe that HUFFERD likely has a sexualized interest in children and depictions of children. I therefore believe that evidence of child pornography is likely to be found on the SUBJECT PHONES.

25. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I believe there is probable cause to believe that the items set forth in Attachment B will be stored on the SUBJECT PHONES for a number of reasons, including but not limited to the following:

a. Once created, electronically stored information (ESI) can be stored for years in very little space and at little or no cost. A great deal of ESI is created, and stored, moreover, even without a conscious act on the part of the device operator. For example, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache," without the knowledge of the device user. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently

viewed Internet pages or if a user takes affirmative steps to delete them. This ESI may include relevant and significant evidence regarding criminal activities, but also, and just as importantly, may include evidence of the identity of the device user, and when and how the device was used. Most often, some affirmative action is necessary to delete ESI. And even when such action has been deliberately taken, ESI can often be recovered, months or even years later, using forensic tools.

b. Wholly apart from data created directly (or indirectly) by user-generated files, digital devices - in particular, a computer's internal hard drive - contain electronic evidence of how a digital device has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating systems or application operations, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible for a user to use such specialized software to delete this type of information - and, the use of such special software may itself result in ESI that is relevant to the criminal investigation. FBI agents in this case have consulted on computer forensic matters with law enforcement officers with specialized knowledge and training in computers, networks, and Internet communications. In particular, to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

26. Based on my training and experience, and my consultation with computer forensic agents who are familiar with searches of computers, I know that in some cases the items set forth in Attachment B may take the form of files, documents, and other data

that is user-generated and found on a digital device. In other cases, these items may take the form of other types of data - including in some cases data generated automatically by the devices themselves.

SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

27. Search Techniques: Searching the SUBJECT PHONES for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement personnel with appropriate expertise may need to conduct more extensive searches, such as scanning areas of the disk not allocated to listed files, or peruse every file briefly to determine whether it falls within the scope of the warrant.

28. Further, in accordance with the information in this Affidavit, law enforcement personnel will execute the search of digital devices seized pursuant to this warrant as follows:

a. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will produce a complete forensic image, if possible and appropriate, of the SUBJECT PHONES. In addition, appropriately trained personnel may search for and attempt to recover deleted, hidden, or encrypted data to determine whether the data fall within the list of items to be seized pursuant to the warrant. In order to search fully for the items identified in the warrant, law enforcement personnel, which may include investigative agents, may then examine all of the data contained in the forensic image/s and/or on the digital devices to view their precise contents and determine whether the data fall within the list of items to be seized pursuant to the warrant.

b. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify,

segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this Affidavit.


c. If, after conducting its examination, law enforcement personnel determine that any digital device is an instrumentality of the criminal offenses referenced above, the government may retain that device during the pendency of the case as necessary to, among other things, preserve the instrumentality evidence for trial, ensure the chain of custody, and litigate the issue of forfeiture.

CONCLUSION

29. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2422(b), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), are located on the SUBJECT PHONES. I therefore request that the court issue a warrant authorizing a search of the items specified in Attachment A for the items more fully described in Attachment B.

Presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

Dated this 15th day of March, 2018.



Gabriel Stajduhar, Affiant
Special Agent, HSI

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on the 16th day of March, 2018.



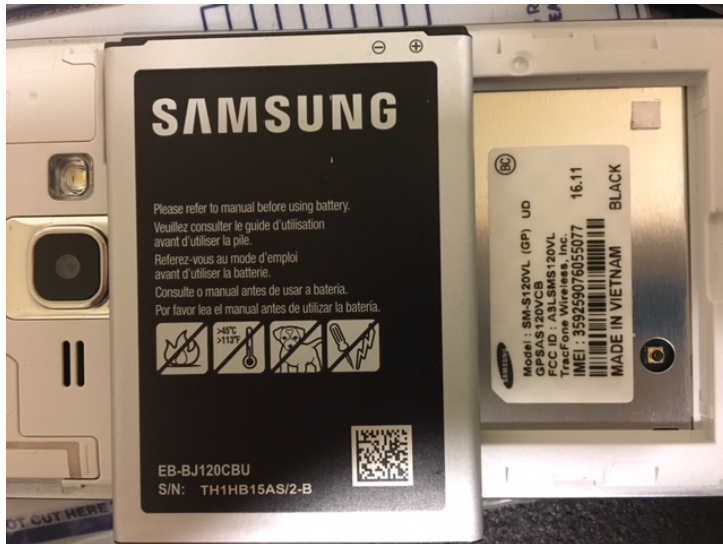
BRIAN A. TSUCHIDA
United States Magistrate Judge

ATTACHMENT A

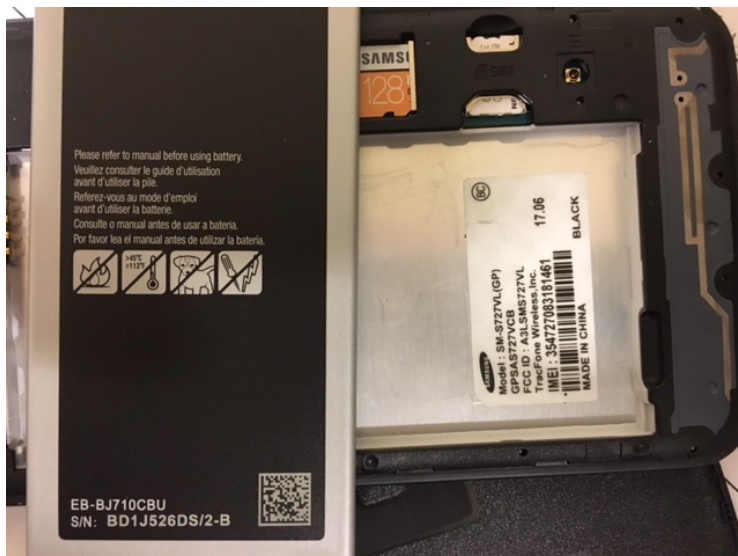
Description of Property to be Searched

Three cellular phones seized from the residence of PETER JAMES HUFFERD on March 9, 2018, and currently in the possession of the United States Probation Office in Seattle, Washington. The cellular phones are further described as follows:

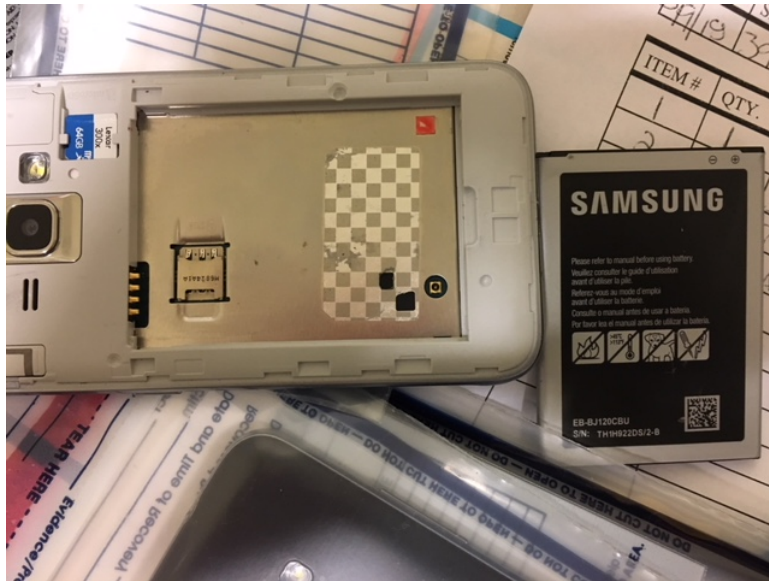
Samsung SM-S120L (IMEI 359259076055077)



Samsung SM-S727VL (IMEI 354727083181461)



Samsung Galaxy (missing identification sticker)



ATTACHMENT B
ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2422(b) (Attempted Enticement of a Minor), 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography), and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography) which may be found on the SUBJECT PHONES:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media.
2. Evidence of the installation and use of P2P software, and any associated logs, saved user names and passwords, shared files, and browsing history;
3. Letters, e-mail, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;
4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;
5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;
6. Any and all evidence related to contact and/or communications with minors;
7. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the SUBJECT PHONES;
8. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the SUBJECT PHONES.
9. Any passwords, password files, test keys, encryption codes or other information necessary to access the SUBJECT PHONES;

10. Evidence of who used, owned or controlled the SUBJECT PHONES at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

11. Evidence of malware that would allow others to control the SUBJECT PHONES such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

12. Evidence of the attachment to the SUBJECT PHONES of other storage devices or similar containers for electronic evidence;

13. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from a digital device;

14. Evidence of times the SUBJECT PHONES were used;

15. Any other information from the SUBJECT PHONES necessary to understand how the digital device was used, the purpose of its use, who used it, and when;

16. Records and things evidencing the use of the Internet including:

- a. Equipment used to connect computers to the Internet;
- b. Records of Internet Protocol (IP) addresses used;
- c. Records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.